УДК: 323.21:004 (575.2)(04)

Сейдакматов Нурман Адисович
кандидат юридических наук
Сейдакматов Нурман Адисович
юридика илимдеринин кандидаты
Seydakmatov Nurman Adisovich
candidate of legal sciences

Каныбекова Бактыгуль Каныбековна,
кандидат юридических наук,
доцент кафедры теории и истории
государства и права Юридического факультета
Кыргызского национального университета имени Жусупа Баласагына
Каныбекова Бактыгуль Каныбековна,
юридика илимдеринин кандидаты, мамлекеттик жана укук теориясы жана тарыхы кафедрасынын доценти
Ж. Баласагын атындагы Кыргыз улуттук университетинин юридикалык факультети
Kanybekova Baktygul Kanybekovna,
PhD in Law, associate Professor of the Department of Theory and History
of State and Law Faculty,
of law kyrgyz national universitynamed after Zh. Balasagyn

МЕТОДОЛОГИЧЕСКИЕ ВОПРОСЫ ПО ПРОТИВОДЕЙСТВИЮ КИБЕРТЕРРОРИЗМУ

Аннотация. В данной статье описаны и раскрыты методологические проблемы противодействия кибертерроризму, наряду с обеспечением информационной безопасности (далее ИБ) в деятельности общества, государства, и отдельных граждан. Также представлены основные положения, понятия и определения, термины, методы обеспечения ИБ, различные виды и источники угроз ИБ, описаны организационно-правовое методологическое обеспечение ИБ деятельности общества и систем по различным направлениям ее жизненного цикла.

Вместе с тем, применение высоких технологий в то же время накладывает и высокую ответственность на владельцев информационных систем, без должного уровня безопасности невозможно гарантировать конфиденциальность вверенных и обрабатываемых данных. Как известно, в условиях активного и масштабного внедрения информационных технологий во все области государственного управления, актуальность данной проблемы возрастает. При этом необходимо сделать акцент на том, что вопросы обеспечения информационной безопасности и проблемы противодействия кибертерроризму не получили концептуального подхода на доктринальном и законодательном уровне, хотя и затрагивается в ряде некоторых документов.

Ключевые слова: методология, информация, информационная безопасность, терроризм, кибертерроризм, антитеррористические действия, международное сотрудничество.

КИБЕРТЕРРОРИЗМГЕ КАРШЫ ТУРУУНУН МЕТОДИКАЛЫК МАСЕЛЕЛЕРИ

Аннотация. Бул макалада коомдун, мамлекеттин жана айрым жарандардын ишмердүүлүгүндө маалыматтык коопсуздукту (мындан ары - ИС) камсыз кылуу менен катар кибертерроризмге каршы туруунун методикалык көйгөйлөрү баяндалган жана ачылган. Ошондой эле маалыматтын коопсуздугун камсыз кылуунун негизги жоболору, түшүнүктөрү жана аныктамалары, мөөнөттөрү, маалыматтык коопсуздуктун коркунучтарынын ар кандай түрлөрү жана булактары келтирилген, коомдун жана анын тутумунун ар кандай чөйрөлөрүндөгү тутумдардын ишмердүүлүгү үчүн маалыматтык коопсуздукту уюштуруучуктук методикалык жактан камсыздоо баяндалган жашоо цикл.

Ошол эле учурда, жогорку технологияларды колдонуу бир эле учурда маалымат тутумдарынын ээлерине чоң жоопкерчиликти жүктөйт, тийиштүү деңгээлдеги коопсуздуксуз, ишенип берилген жана иштетилген маалыматтардын купуялуулугуна кепилдик берүү мүмкүн эмес. Белгилүү болгондой, мамлекеттик башкаруунун бардык чөйрөлөрүнө маалыматтык технологияларды жигердүү жана масштабдуу киргизүү шартында, бул көйгөйдүн актуалдуулугу жогорулайт. Ошол эле учурда, маалымат коопсуздугун камсыз кылуу маселелери жана кибер терроризмге каршы туруу маселелери доктриналык жана мыйзамдык деңгээлдерде бир катар документтерде козголгонуна карабастан, концептуалдык мамилеге ээ болбогонун баса белгилеп кетүү керек.

Негизги сөздөр: методология, маалымат, маалымат коопсуздугу, терроризм, кибертерроризм, антитеррордук иш-аракеттер, эл аралык кызматташтык.

METHODOLOGICAL ISSUES IN COUNTERING CYBER TERRORISM

Abstract. This article describes and discloses the methodological problems of countering cyber terrorism, along with ensuring information security (hereinafter IS) in the activities of society, the state, and individual citizens. It also presents the main provisions, concepts and definitions, terms, methods of ensuring information security, various types and sources of information security threats, describes the organizational and legal methodological support of information security for the activities of society and systems in various areas of its life cycle.

At the same time, the use of high technologies at the same time imposes a high responsibility on the owners of information systems; without the proper level of security, it is impossible to guarantee the confidentiality of entrusted and processed data. As you know, in the conditions of active and large-scale introduction of information technologies in all areas of public administration, the urgency of this problem increases. At the same time, it is necessary to emphasize that the issues of ensuring information security and the problems of countering cyber terrorism have not received a conceptual approach at the doctrinal and legislative level, although they are touched upon in a number of some documents.

Key words: methodology, information, information security, terrorism, cyber terrorism, anti-terrorist actions, international cooperation.

В настоящее время человечество выступает участником формирования глобального информационного общества. За последние годы произошли серьезные изменения в сфере использования информационных технологий, что послужило более пристально обращать внимание на проблемы возникающие в сфере обеспечения информационной безопасности, а также рассмотрения вопросов противодействия кибертерроризму. Существующие решения направлены на реализацию определенных задач и не являются тем механизмом, который выступает регулятором взаимодополняющих и взаи-

модействующих друг другу элементов, обеспечивающих соответствующий уровень информационной безопасности.

Активное развитие информационных технологий и информационных отношений требует серьезного внимания со стороны государства, а именно его специальных органов.

Актуальность сферы по противодействию кибертерроризму органами ГКНБ Кыргызской Республики определяется еще и эффективностью обеспечения комплексных контрразведывательных и иных специальных мер, направленных на выявление, предупреждение и пресечение данных угроз. Непрерывное разведывательное отслеживание, анализ, оценка и прогноз динамики развития негативных факторов информационного характера в глобальном пространстве, формирующих угрозы, как национальной безопасности, так и региональной безопасности в целом, ставит перед органами ГКНБ особые задачи, решение которых требует не только практической деятельности, но и теоретических исследований.

В связи с этим, возникает необходимость в проработке ряда мероприятий, направленных на подготовку специалистов в области обеспечения информационной безопасности, а также изучения методических и нормативно-правовых проблем обеспечения национальной безопасности в данной сфере.

В перспективе в рамках начатых мероприятий можно рассмотреть различные варианты деятельности органов ГКНБ в сфере оперативной, оперативно-технической и иной контрразведывательной деятельности по обеспечению информационной безопасности и развитию информационных технологий Кыргызской Республики. Это обусловлено усиливающейся необходимостью эффективной подготовки соответствующей категории специалистов, их мотивирования и реализации конкретных задач, стоящих перед органами национальной безопасности.

Также хотелось бы отметить о межгосударственных информационных конфликтах, которые возникают в сфере обороны, основной категорией которой выступает информационная война в различных сферах применения информационных технологий, для того чтобы незаконно использовать существующие информационные ресурсы различными террористическими группировками или же криминальными структурами. При этом необходимо обеспечить защиту прав граждан для получения достоверной информации, а также обеспечить защиту самой информации представляющую личную безопасность.

Основными причинами недостаточного развития системы по обеспечению информационной безопасности следует назвать следующее:

- законодательная основа по обеспечению информационной безопасности не содержит всех тех существующих проблем, а в некоторых случаях носит и противоречивый характер;
- недостаточное финансирование;
- не создаются в нужных объемах сертифицированные средства защиты информации, включая прикладные программные средства и высококачественные операционные системы защиты;
- слабая координация деятельности по противодействию кибертерроризму органов государственной власти в регионах;
- недостаток квалифицированных специалистов в области информационных технологий.

Для того, чтобы эффективно работала система по противодействию кибертерроризму нужна обязательная согласованность между экономическими, технологическими, правовыми и организационными факторами для обеспечения необходимого уровня информационной безопасности.

Понятие информационной безопасности рассматривается правоведами по-разному, одни говорят, что информационная безо-

пасность – это совокупность информационных аппаратов и программ для того, чтобы обеспечить защиту информации, а другие утверждают, что это обеспечение защиты потребностей граждан или же всего общества в целом.

Если рассматривать понятие информационной безопасности в широком смысле, то это есть обеспечение защиты информационной среды общества, которая формируется и организуется в интересах граждан, организаций и государства в целом.

Главной причиной возникновения проблем в обеспечении защиты информации выступает отсутствие четко прописанной политики по обеспечению информационной безопасности, которая содержала бы в себе финансовые, технические и организационные решения с последующей организацией контроля в их оценке и реализации.

Поэтому нужно включить в систему регулирования данного вопроса четко установленные действия экономического и организационного характера, которые могли бы повысить уровень достижения поставленных задач.

В связи с быстрым ростом развития информационных технологий (ИТ) в общем и обеспечения информационной безопасности, как науки, нужно в срочном порядке создать соответствующие методы для организации эффективных мер по противодействию кибертерроризму.

В настоящее время поддержания мира, это не только материальная база, которая выступает предметом жёсткого соперничества между собой, а всё-таки ключ к успеху и процветанию каждого государства лежит и в умении управлять информационными возможностями и ресурсами. Нужно также отметить, что современное общество в большинстве случаях свободна от национальных границ, а также во всех сферах деятельности существуют новейшие функциональные возможности, основой которого является Интернет. Это международные компании, суперсовременная электронная экономика и конечно же научный коллектив, который работает совместно над одной проблемой, тем временем находясь в разных уголках мира. Параллельно с положительными возможностями человечество столкнулось и с отрицательной стороной развития и применения информационных технологий, это когда Сетевые структуры явились основой международной преступности, включая информационные войны и кибертерроризм.

Нужно также отметить, что в современный период в борьбе за политическое и экономическое влияние на международной арене применяются не вооруженные силы, а начали использовать скрытую форму управления и контроля с применением информационных ресурсов государств.

В современном мире, когда человечество столкнулось с новыми вызовами и угрозами, к которым он не был еще готов, особая актуальность возникает в деятельности, которая сможет обеспечить безопасность человека, то есть безопасность в широком смысле, содержащая все сферы жизнедеятельности человека.

В далекие 80 годы, по телефону могли получать только одну страницу информации в секунду, а в настоящее время с помощью тонкой нити оптического волокна можно передать более 90 тысяч томов в секунду. Также в эти годы для хранения информации в размере одного гигабайта нужна была целая комната, а сейчас 200 гигабайт дискового пространства можно поместить просто в кармане. Не менее важным стало низкая стоимость передачи информации, которая позволяет снизить входной барьер. Из-за того, что вычислительные машины стали дешевыми и размер компьютеров и других портативных устройств в разы уменьшились, переходя до уровня смартфонов, результаты децентрализации стали более серьёзными.

В итоге, мировая политика больше не выступает только правительственной сферой деятельности. Организации, частные лица, а также Wiki Leaks, неправительственные организации, международные корпорации, спонтанные социальные движения и тер-

рористические организации тоже получили такие возможности, то есть играть определенную роль в мировой политике.

Таким образом, нужно отметить, что положительными процессами применения информационных технологий и глобальной информатизацией, происходят и отрицательные процессы, связанные с криминализацией и милитаризацией информационного пространства.

Мировые информационно-кибернетические технологии и информационно-телекоммуникационные системы в настоящее время выступают высокоэффективным средством и оружием для достижения целей военно-политического, террористического и криминального характера. Поэтому нужно в срочном порядке человечеству создать, и реализовать новые механизмы для обеспечения безопасности в информационном пространстве, то есть для противодействия новым угрозам. Так как новые угрозы имеют трансграничный и транснациональный характер, наиболее важными средствами борьбы с ними будет разработка новых международно-правовых механизмов по обеспечению информационной безопасности. При рассмотрении проблем противодействия кибертерроризму, нужно различать и другие угрозы безопасности. Но тем не менее применение мировых информационно-коммуникационных систем как механизма планирования и управления осуществления террористических актов не может относиться к кибертерроризму. Главной особенностью кибертерроризма выступает применение информационно-телекоммуникационных систем как оружия для совершения террористических актов. Поэтому основным элементом кибертерроризма выступает кибернетическая атака.

Но кибератаки могут проводиться и в других целях, например, спецслужбами в военно-политических целях, а также хакерами в хулиганских или криминальных целях. При этом проводимые кибератаки в различных целях с технической точки зрения не могут быть отличены – в сети, в компьютере, в канале, он может проявиться только в случае уровня мастерства, атакующего или же при эффективности используемых средств.

При изучении информационно-коммуникационных технологий с точки зрения безопасности важную роль играет их двойственность: во-первых, применение информационно-телекоммуникационных технологий, может стать как объект нападения, а во-вторых может выступать как оружие в руках террористических группировок, преступников или противников, а иной раз эти технологии и системы могут быть применены одновременно как-то и другое. Собственно, из-за чего трудно будет провести грань между применением информационно-коммуникационных технологий в военно-политическом противодействии, в кибертерроризме, а также в других видах киберпреступности.

Кибертерроризм отличается от других форм преступных воздействий на информационную среду прежде всего своими целями, которые свойственны терроризму вообще. Террористы и террористические организации стремятся к тому, чтобы их теракты: имели опасные последствия; стали широко известны населению; имели большой общественный резонанс; создали атмосферу угрозы непредсказуемого повторения теракта.

Угроза катастроф мирового масштаба в случае, если террористы удачно провернут кибератаку, то мировому сообществу необходимо будет согласованно в срочном порядке принять меры против таких угроз. По существу, сегодня уже начата работа по созданию нового международно-правового режима, объектом которого выступают информационно-коммуникационные технологии, сама информация и механизмы его использования. Немаловажную роль в таком случае имеет проблема по разработке единого понятийного аппарата, где должны быть прописаны единые термины, которые применяются в это специальной сфере, а также необходимо стремиться к согласованию законодательной базы в части борьбы с

кибертерроризмом и киберпреступлениями вообще.

Неординарность новых угроз безопасности киберпространства может потребовать от международного сообщества и неординарных мер противодействия. Одной из таких мер может стать использование потенциала хакерского сообщества в антитеррористических целях. При этом мы трактуем хакерство не только как сообщество киберхулиганов и киберпреступников, а шире - как сообщество людей с ярко выраженным (иногда и гипертрофированным) увлечением к познанию в области информационных технологий, выходящим за рамки познавательной и учебной деятельности. Для привлечения таких неформальных сообществ к борьбе с международным кибертерроризмом необходимо обратить самое серьёзное внимание на выработку позитивной мотивации одарённой молодёжи. В мотивах действий хакеров психологи выделяют: любопытство; удовольствие, получаемое от ощущения силы; узнавание в киберпространстве таких же, как ты; переживание опыта потока, т. е. особого психологического состояния включенности в деятельность, при котором действия и их осознание сливаются для субъекта в одно целое, а результат деятельности отходит на задний план.

Все эти мотивы могут иметь для общества как положительную, так и отрицательную направленность. Поэтому, необходимо привлечь психологов, педагогов, социологов, специалистов mass-media для разработки систем мер, направленных на положительную ориентацию «кибернеформалов». Задача формирования представлений о добре и зле, «моральных заповедей» поведения в киберпространстве психологически не проста. Опосредованность, разделение во времени и пространстве приводит к сильному изменению представлений об антигуманности тех или иных действий в киберпространстве: сидя за монитором компьютера, человек отстранён от последствий и непосредственно не наблюдает того ущерба, который он наносит своими преступными действиями другим людям.

Считаем важным разработать систему мер по мониторингу и контролю за распространением знаний и технологий, критичных с точки зрения информационной безопасности. Один из основных ресурсов, требующих мониторинга, - это высококвалифицированные специалисты, обладающие знаниями в области высоконадёжных методов защиты информации. Именно они являются объектом интереса деструктивных элементов, в том числе по заказам международных террористических организаций.

Постоянных усилий требует также работа по согласованию взаимоприемлемых условий функционирования сети международных центров по предупреждению и противодействию кибератакам. Необходимо выработать работоспособные механизмы обмена опытом в этой области.

При современном уровне развития высоких технологий расширяются возможности их использования для совершения террористических действий.

На сегодняшний день большинство государств ведут активную работу по изучению потенциальных случаев таких проявлений, а также созданию мер в борьбе с такими преступлениями. Всемирное киберпространство основным элементом которого выступает Интернет рассматриваются, как допустимое благоприятное поле для террористической деятельности. Уместно отметить, что компьютерный терроризм и соответствующая ему деятельность по целям и сути своей имеют смысл именно в рамках использования для этого крупной сетевой инфраструктуры или контроля над распределенными в сети важными информационными ресурсами. Данное обстоятельство указывает на типы сетевых объектов и инфраструктуры, которые следует рассматривать в качестве первоочередных объектов атаки террористов на Киберпространстве. Несмотря на пристальное внимание к отмеченным вопросам («кибертерроризм» или «компьютерный терроризм»), в имеющихся документах национального и международ-

ного уровня, не обнаружены конкретные результаты исследования об обязательных активных действиях в борьбе с ними. Это можно будет объяснить, во-первых, тем, что характер проблемы в данной сфере комплексная и объемная, а также отсутствует отработанный методологический подход. А во- вторых, это указывает на то, что недостаточно глубоко понимаем актуальной этой проблемы, и об отсутствии со стороны государственных ведомств необходимых мер для борьбы с такими видами преступлений.

С учетом вышеизложенного, в рамках основных положений попробуем в данной статье кратко изложить основные понятия формы атаки (феномен, явления), признаки которой можно истолковывать как кибертерроризм, а также представить модель защиты (противодействия), как механизм по пресечению или предупреждению таких противоправных действий. Можно в нескольких словах сформулировать основные положения для разработки форм защиты и системных мер.

Кибертерроризм – это совокупность незаконных действий, связанных с применением искажённой информации для нагнетания страха и напряженности, посягательство на материальные объекты, жизнь людей путем угрозы или другими видами неправомерных действий для того чтобы получить превосходство в решении политических, экономических и социальных проблем. Направление злоумышленных и противозаконных действий на сетевой среде с целью использования их результатов для проведения террористических актов могут быть следующие:

- разрушение системы национального или международного масштаба путем уничтожения системы управления или отдельных его подсистем;
- незаконный доступ к сетевой, а также секретной информации, нарушение его целостности и защищенности;

Также нужно различать действие террористов от террористических действий с применением Интернет ресурсов в целях распространения своих взглядов, обострения напряженности и страха среди общества.

Чтобы подчеркнуть отличие информационной безопасности от антитеррористической информационной безопасности, рассмотрим данное понятие.

Антитеррористическая информационная безопасность – это совокупность механизмов, действий, мер, а также инструментальные пути и средства, с помощью которых можно раскрыть и предотвратить неправомерные действия, которые могли бы привести к уничтожению или разрушению информационной системы, путем вывода ее из строя, а также получения доступа к охраняемым законом информациям обладающими степенью секретности, нарушая тем самым ее защищенность и целостность.

Фундаментом антитеррористических действий с применением сети Интернет является традиционная информационная безопасность, его механизмы, методы, формы и инструментальные средства. Создание и построение механизмов информационной безопасности для определенных изделий, продуктов и комплексов в сетевой среде, а именно в сети Интернет –многоплановая и очень сложная задача. Для ее решения необходимы четко разработанные механизмы и средства их реализации в определенной степени этой деятельности, например, в законодательной, программно-технической, административной и операционной сфере. Но уровень реализации таких мер и механизмов у каждого государство свой и отличается друг от друга разными факторами (степень развития информационной инфраструктуры, научно-технической базой, финансированием и др.). Говоря о традиционной информационной безопасности которая выступает фундаментом антитеррористической информационной безопасности следует подчеркнуть, что деятельность по пресечению или предупреждению террористических актов в сети Интернет и в информационной среде имеет свою особенность. Для создания рациональной программы действий специалистов по формированию единой политики безопасности и поэтапно-

го его внедрения нужны характеризующие ее факторы.

Сформулируем в общем положения, которые будут рассматриваться как отправные (начальные) для создания механизмов атаки, которые могут быть охарактеризованы как кибертерроризм. Изучая определенный сценарий террористических действий с применением сети Интернет в самой действующей постановке в качестве взаимодействующих способов,_характеризующих «типовой профиль» такого понятия можно выделить следующие:

- субъект действия - персона и (или) группа лиц, имеющих целью проведение террористических действий против объекта (объектов), и (или) совокупность их агентов в сетевой среде осуществление атаки с помощью применения секретных каналов передачи информации;
- предмет действия - сетевая инфраструктура (физическая среда передачи данных, коммуникационные средства и программное обеспечение), предоставляющие доступ к информационно-вычислительным ресурсам системы;
- цель действий - использовать предмет действия (сетевую инфраструктуру) для разрушительного воздействия на объекты, с отрицательными последствиями (например, шантаж, покушение на жизнь людей, уничтожение вторичных объектов и др.).
- первичный объект- компьютерная программа для более узкой, но более важной или, например, способной прямо влиять на здоровье людей, области применения;
- вторичный объект – люди или группа людей, информационные системы, различные материальные объекты, на которых могут воздействовать первичные объекты, вплоть до уничтожения;

Стандартный сценарий действий террористических группировок при этом должен будет как правило содержать:

- действия, предоставляющие неавторизованный доступ к секретной информации;
- уничтожение, модификацию или замену программного кода, обеспечивающего нормальное (регламентированное) функционирование системы;
- снижения доступа внутренних и внешних агентов системы безопасности, которое могут оперативно предотвратить злоумышленные действия.

Конечно, представленные положения не позволяют сформулировать модель атаки с надлежащей степенью полноты. Это предмет более глубокого анализа специалистов разных (в том числе гуманитарного цикла) направлений. Однако, и они позволяют описать основные типы угроз, предсказать условия их реализации, а значит, и общие соображения, которые могут быть положены в основу модели противодействия атаке. Следует отметить, что налицо комбинация всех трех типов угроз, соответственно, - конфиденциальности, целостности и доступности, на предотвращение которых должны быть ориентированы системы информационной безопасности рассматриваемых комплексов. Важным фактором эффективности противодействия выступает необходимость оперативной, в реальном времени реакции на последовательность вышеперечисленных действий с атакующей стороны.

Рассматривая общие положения модели защиты, как системы контрмер, которые необходимо предпринимать на всех уровнях реализации сетевой безопасности для предотвращения каждой из перечисленных выше угроз и их совокупности в контексте «среднего» сценария террористического акта. Главной задачей на административном уровне является выработка подходов к формированию политик безопасности для распределенных, вообще говоря, гетерогенных систем, интегрирующих в своем составе подсистемы с различными функциями и условиями эксплуатации.

В числе первых действий на операционном, а тем более, программно-коммуникационном уровне обеспечения информационной безопасности, должно быть выработано (в рамках изучения базовых положений, современных критериев оценки безопасности информационных технологий) профилей защиты и заданий на обеспечение безопасности, которые отвечали бы политике безопасности систем, подлежащих защите от кибертеррористических атак. Как результат более эффективных мер, которые будут способны противодействовать угрозе конфиденциальности, то есть незаконному доступу к секретной информации, могут рассматриваться:

- на операционном уровне - это обучение и управление персоналом, четкое распределение обязанностей и минимизация привилегий;
- на программно-техническом уровне - средства идентификации и аутентификации пользователей, учитывающие их индивидуальные особенности; управление ресурсами на основе комбинации традиционных и новейших моделей логического разграничения доступа, учитывающих различные требования по безопасности к разным компонентам системы, а также криптографическая поддержка и экранирование.

Хотелось бы отметить, что приведены не все основные меры, способные противодействовать перечисленным угрозам. Их сложно систематизировать и обобщить в одной статье. Поэтому отметим мероприятия, обобщающие их в рамках отдельных уровней. К мерам общего характера на этом направлении можно отнести следующие:

- разработка новых законодательных актов (национальных и международных) в области контроля над использованием систем сетевого управления национально значимыми сферами оборонной промышленности и бизнеса с точки зрения возможного применения в отношении них террористических действий.
- поиск типовых подходов к формированию – политик безопасности для стратегически важных объектов, управление которыми осуществляется с использованием сетевых структур, на основе анализа рисков, связанных с террористическими действиями (актами);
- строгое следование требованиям и критериям стандартов (национальных и (или) международных) оценки продуктов или систем, предназначенных для эксплуатации в сетевой среде в условиях определяющих быструю реакцию на действие террористов;
- развитие уже существующих стандартов в этой области на основе проведенного анализа.

Однако темпы роста мегасети Интернет огромны. Сегодня она объединяет более 200 млн. сетевых ЭВМ в почти 250 странах мира на всех континентах. Эта сеть «де-факто» или потенциально имеет связность с любыми сетями от локальных бытовых и исследовательских до сетей силовых ведомств или сетей, которые используются для управления национально значимыми отраслями или сферами деятельности. Это безусловно инфраструктура, которая потенциально может быть задействована террористическими организациями для реализации своих целей в каждой из перечисленных выше сфер и отраслей человеческой деятельности. Более того, чем выше уровень развития сетевых технологий, шире спектр их использования в различных сферах человеческой деятельности, тем вероятнее внимание к ним со стороны террористов и более изощрены могут быть их действия.

На сегодняшний день, например, не будет выглядеть особенным отказ от бортовой системы управления транспортным средством в воздухе, на воде, на земле, воздействие на управление, которое может перенацелить боевые снаряды (ракеты) на другие цели. К сожалению, такие примеры можно

продолжить. Это нужно понимать и предотвращать такие действия.

Представленные в статье идеи и положения следует рассматривать как_результат осознания очень трудной и особенной для решения проблемы. Исходная посылка о том, что в методическом плане традиционные подходы к_созданию и реализации системы обеспечения информационной безопасности не меняются, а при формировании систем и способов противодействия кибертерроризму также остаются, то есть эти системы не только будут отменены, а наоборот они требуют более конкретного подхода к его решению.

В связи с этим совершенствование основной идеи обеспечения безопасности информационных технологий, разработка новых конструктивных моделей для тестирования, сертификации средств защиты сложных компьютерных систем, создание доказательной базы, улучшение программно-технической базы по обеспечению безопасности – это и есть правильное направление в настоящее время. Однако трудности на этом пути есть. Большинство национально значимых информационных систем между собой взаимосвязаны в рамках нынешних магистральных сетевых инфраструктур, что рассматривается как потенциально уязвимым для кибертерроризма. Значит те государства, у которых слабо развита сетевая инфраструктура более подвержена внешним угрозам или террористическим атакам. Поэтому больше всего крупные террористические атаки осуществляются или готовятся в том государстве где слабо развита сетевая инфраструктура.

Подводя итоги можно отметить, о том, что проблема обеспечения информационной безопасности (в том числе сетевой) более сложная и специфическая. Она, кроме общих (в методологическом, техническом, правовом и т. п. плане) межнациональных, затрагивает и национальные интересы. Поэтому их реализация требует серьезно проработанные программы и механизмы. И этот факт, что такие новые разработанные программы обязательны, сомнений не вызывает и это прекрасное поле для активных совместных действий на международной арене.

Список использованных источников и литературы

1. *Алексенцев А.И.* Сущность и соотношение понятий «защита информации», «безопасность информации», «информационная безопасность» //Безопасность инф. технологий. М.,1999. №1. С. 15.

2. *Арабаев Ч.А., Омукеева Н.А.* Право интеллектуальной собственности Кыргызской Республики. Бишкек. 2004.

3.*Гуменюк А.Д., Новокшанов О.Н.* Основы построения и безопасности функционированию телекоммуникационных систем. Курс лекций. М., 2008.

4. *Карпов В. И.* Теоретические основы обеспечения безопасности личности, общества и государства: учеб. пособие; изд. 2-е доп. и перераб. /В. И. Карпов, О. Н. Новокшанов, Д. Б. Павлов. – М.: Юридический институт МИИТа, 2010. – 236 с.

5. *Кириленко В.И., Новокшанов О.Н., Обухов А.Н.* Теоретические основы государственно-правового регулирования информационных правоотношений. Монография. М., 2009.

6. *Копылов В.А.* Информационное право. Вопросы теории и практики. М.: Юрист, 2003. С. 43.

7.*Оторова Б.К.* Правовое регулирование информационно-правовых отношений в Кыргызской Республике: автореф. дис. ... канд. юрид. наук: 12.00.01. Б., 2012.

8.*Семененко В.А.* Информационная безопасность: учебное пособие. 2-е С3Оизд., стереот. М.: МГИУ, 2005. 230 с.

9.*Сейдакматов Н.А.* Безопасность личности, общества и государства // Известия Национальной Академии Наук Кыргызской Республики. 2012. № 2. С. 144-149.

10.*Сейдакматов Н.А.* Безопасность информации как состояние ее защищенности // Вестник Кыргызско-Российского Славянского университета. 2012. Т. 12. № 12. С. 49-52.

11.*Темирбаев К.Т., Сагынбаев А.А., Джаркеев А.Н., Кадыралиев Т.Н.*.Информационная безопасность Кыргызской Республики/ Бишкек, 2007. С. 11.